OBEDIENCE GLOBAL LTD

Data Processing Agreement

The Article 28 processor terms under which we handle customer project data.

Version 1.2 | Effective 28 July 2026 | Privacy & data

Owner Obedience Global Ltd board | Approved by Obedience Global Ltd board on 28 July 2026
Approval state company-approved | Next review 28 October 2026

01 Roles

For personal data inside your QuantifyQS workspace, you are the controller and Obedience Global Ltd is your processor. Obedience remains a separate controller for its own account administration, security, billing, legal-compliance and business records. This DPA forms part of the QuantifyQS Terms of Service and reflects Article 28(3) UK GDPR.

02 Processing details

Item | Scope | Duration

Subject matter and purpose | Hosting and operating the QuantifyQS workspace features selected by the customer, including storage, calculation, export, support and customer-approved assistance | For the service term and the deletion periods below

Nature of processing | Collection, transmission, organisation, storage, retrieval, calculation, display, export, restriction, backup and deletion on the customer's documented instructions | Continuous while the relevant feature is used

Data subjects | Customer users, staff, clients, suppliers, consultants and other people whose data the customer lawfully enters into a workspace | Determined by the customer and the service term

Personal data | Account identifiers, contact and role data, project correspondence, document metadata, commercial records and other workspace fields chosen by the customer | Determined by the customer, subject to this DPA and the Retention Schedule

Special-category and criminal-offence data | Not approved for routine use. The customer must not submit it unless a separate written assessment, lawful basis, instructions and safeguards are agreed first | No current approved processing period

03 Documented instructions

The Terms, this DPA, the customer's configuration and ordinary authorised use of the product are the documented instructions. We will tell the customer if an instruction appears to infringe applicable data-protection law, unless law prohibits that notice. A materially different purpose, new high-risk data category or confidential hosted-model workflow needs written instructions and the relevant change assessment before processing starts.

04 Our processor commitments

- Process customer data only on documented instructions, including the product use described above
- Ensure everyone with access is bound by confidentiality
- Apply the technical and organisational measures in our Security Overview: encryption in transit and at rest, tenant isolation enforced at the database (row-level security), least-privilege access, daily encrypted off-site backups
- Use processors and subprocessors only from the published Service Provider and Subprocessor List, impose equivalent data-protection duties, and give at least 14 days' notice of a material new customer-data subprocessor with a reasonable objection route
- Help you respond to data-subject rights requests and, where you cannot resolve them alone, regulatory

enquiries

- Tell you without undue delay about any personal data breach affecting your data
- Delete or return data at contract end under the system-specific periods below, with export available first
- Make available the information needed to demonstrate compliance, and permit audits within reasonable bounds

05 Return, deletion and legal holds

The customer may request an export before termination. Active Quantify workspace and project records are scheduled for deletion within 30 days after verified termination or instruction. Encrypted backups then age out within the rolling 30-day window and must not be restored into active use without reapplying the deletion. Authentication-provider copies can take up to 90 days after termination under the current provider terms.

We may retain the minimum data required by law or a narrowly scoped legal hold. That data is isolated, access-restricted and not used for another purpose. The customer remains responsible for retaining any export it needs after the service ends.

06 International transfers

Primary structured project records are stored in the United Kingdom. File objects currently report a Western Europe automatic location, and supporting identity, hosting, email, monitoring and approved AI paths can process data in the EEA, United States or through a global network. Where required, the relevant provider terms use UK adequacy, the UK Extension to the EU-US Data Privacy Framework, or the UK Addendum or IDTA with the EU Standard Contractual Clauses. Account-specific entity, location and transfer evidence is maintained internally and reviewed before higher-risk processing.

07 Audit and assistance

We provide information reasonably needed to demonstrate compliance and assist with rights, security, breach assessment, DPIAs and regulator consultation, taking account of the processing. Ordinarily the parties use current security material and independent provider reports first. A customer audit requires reasonable notice, confidentiality, a scope relevant to its data and no avoidable risk to another tenant. The once-per-year limit does not apply after a relevant breach or where a regulator or applicable law requires more.

08 Signed copies

A countersignable copy of this DPA for your procurement records is available on request: hello@obedience.global.

Canonical online record: https://obedience.global/policies/data-processing